

### **REMARKS**

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is directed to non-statutory subject matter under the provisions of 35 U.S.C. §101 or is anticipated under the provisions of 35 U.S.C. §102. Thus, the Applicants believe that all of these claims are in allowable form.

#### **I. REJECTION OF CLAIMS 1-2 UNDER 35 U.S.C. § 101**

Claims 1-2 stand rejected under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter. The Applicants respectfully traverse the rejection.

Claim 1 clearly recites that "at least one of: the receiving, the identifying, the updating a threshold similarity, the updating a similarity expectation, the comparing, the associating, or the defining is performed by a processor" (emphasis added). As such, independent claim 1 clearly recites a method that is tied to a particular machine or apparatus (*i.e.*, a processor) that performs at least one of the recited steps. Nevertheless, the Examiner submits that "the device or machine represents merely extra-solution activity, as part of a preamble" (Final Office Action, Page 4). The Applicants respectfully disagree.

First, the Applicants note that the "Interim Examination Instructions For Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101," effective August 24, 2009, define "extra-solution activity" as "activity that is not central to the purpose of the method invented by the applicant" (Interim Examination Instructions, Page 6). The Applicants note that the amendments that were previously made to independent claim 1 in order to comply with 35 U.S.C. § 101 did not include additional steps or activities. Instead, these amendments clarified the manner in which the existing steps or activities are performed (*i.e.*, in at least one case, using a processor). Moreover, the Applicants submit that all of the existing steps and activities are central to the purpose of the claimed method. Specifically, all of the steps of the claimed method are central to the purpose of organizing intrusion detection system alerts indicative of attacks or anomalous incidents into alert classes. Thus, the Applicants respectfully submit that independent claim 1 does not include "extra-solution activity."

Second, the Applicants note that the "device or machine" (*i.e.*, the claimed

processor) is not recited as part of the preamble, as alleged by the Examiner. The claimed processor is clearly recited in the body of independent claim 1, and, as such, constitutes a positive limitation on the scope of the claim.

Third, the Interim Examination Instructions provide that a process comprising "an act, or a series of acts or steps that are  tied to a particular machine or apparatus " constitutes patent-eligible subject matter (See, Interim Examination Instructions, Page 1, "Subject Matter Eligibility"). The Applicants note that the Interim Examination Instructions do not require that every step of a claimed method be tied to a particular machine or apparatus. As clearly recited in claim 1,  at least one of the recited steps is performed by a processor . Thus, the claimed process includes at least one step that  cannot  be "performed by a person alerting another person via a shout, for example, or via mental steps in comparing one alert with another," as suggested by the Examiner (Final Office Action, Pages 4-5). As such, the Applicants respectfully submit that independent claim 1 clearly satisfies the requirements set forth in the Interim Examination Instructions with respect to the patent eligibility of a process. As such, the Applicants respectfully submit that independent claim 1 is directed to subject matter that is statutory within the meaning of 35 U.S.C. § 101.

Claim 2 depends from independent claim 1 and recites at least all of the features recited in independent claim 1. As such, and at least for the reasons stated above with respect to independent claim 1, the Applicants respectfully submit that claim 2 is also directed to subject matter that is statutory within the meaning of 35 U.S.C. § 101.

Finally, the Examiner suggests that because the Applicants amended independent claim 1 in response to the previous Office Action that "it appears that Applicant did not feel claim 1 was sufficiently statutory" (Final Office action, Page 5). The Applicants respectfully submit that independent claim 1 was amended merely to advance prosecution, and that such amendment is in no way an admission as to the statutory status of independent claim 1.

In light of the above, the Applicants respectfully submit that claims 1-2 fully satisfy the requirements of 35 U.S.C. §101. Accordingly, the Applicants respectfully request that the rejection of claims 1-2 under 35 U.S.C. §101 be withdrawn.

## **II. REJECTION OF CLAIMS 1-2, 7-8, AND 13-14 UNDER 35 U.S.C. § 102**

### **A. Claims 1-2, 7-8, and 13-14**

Claims 1-2, 7-8, and 13-14 stand rejected as being unpatentable over the Nine et al. patent (U.S. 6,560,611, issued May 6, 2003, hereinafter "Nine"). The Applicants respectfully traverse the rejection. Specifically, the Applicants submit that Nine fails to teach, show, or suggest several of the features recited in Applicants' independent claims 1, 7, and 13, including:

#### **1. "Comparing the new alert with the one or more existing alert classes"**

The Applicants submit that Nine is completely devoid of any teaching, showing, or suggestion relating to the comparison of an alert (indicating an attack or anomalous incident) – or more specifically, the comparison of features of the alert - to the features of existing alert classes, in order to classify the alert, as claimed by the Applicants in independent claims 1, 7, and 13.

By contrast, Nine teaches a network monitoring system that simply reports a detected problem to the proper individual (e.g., technician), based on the nature of the problem. That is, Nine does not classify the detected problem (e.g., in accordance with its features) by comparing it to known problems, but simply evaluates the detected problem as a discrete incident and reports it to a human technician for further action.

Specifically, Nine teaches a remote monitoring system (RMS) that reports to a network operation site (NOS) when the RMS detects an anomaly with respect to a service it monitors. The report provided by the RMS is a ticket or data record containing information about the service (e.g., location, severity of problem, time of occurrence). In addition, the system "determines the nature of the problem, and notifies the proper personnel [e.g., a technician]" (See, Nine at column 3, lines 25-27). The Examiner alleges that this amounts to "a comparison of an alert in order to classify the alert" (Final Office Action, Page 3). The Applicants respectfully disagree.

The Applicants note that Nine does not explicitly disclose that the process of determining where to place a pending ticket includes a comparison or classification step. In fact, Nine is rather vague in explaining how the proper location for the ticket is determined. At best, Nine discloses an example wherein an accounting engine is

"queried" for the location with the IP address and port number of a nonresponsive service. However, Nine does not disclose that "querying" involves comparing or classifying, much less what might be compared in such a case. It requires a significant intuitive leap to suggest that deciding where to place a ticket is the same as classifying the pending ticket by comparing it to other pending tickets. There are many possible ways in which the proper location for a pending ticket could be determined. Nine appears to disclose determining where to place a pending ticket based on information contained in the pending ticket (e.g., IP address or port number; See, Nine, column 8, lines 41-43); nothing in Nine even alludes to the possibility that information contained in other tickets may be useful in determining where to place the pending ticket.

Thus, there is simply no support in Nine for the step of comparing a pending ticket to other tickets for classification purposes.

**2. "Updating a threshold similarity requirement for one or more of the similar features" and "Updating a similarity expectation for one or more of the similar features"**

The Applicants submit that Nine is completely devoid of any teaching, showing, or suggestion relating to "updating a threshold similarity requirement for one or more features" of an alert relative to features of alert classes or to "updating a similarity expectation for one or more features" of an alert relative to features of alert classes, as claimed by the Applicants in independent claims 1, 7, and 13. The first portion of Nine that the Examiner cites to teach these features in fact merely teaches that the monitoring software is replicated for each service on a device by an informer engine executing forker software and sender software (See, e.g. Nine at column 5, line 45 – column 6, line 9). There is no discussion of examining the features of an alert, or of the need to update a threshold similarity requirement or a similarity expectation for the features of the alert to the one or more alert classes. Nine simply copies software.

The second portion of Nine that the Examiner cites to teach these features in fact merely teaches that information from the ticket file may be extracted and used to generate a report that helps to "detect patterns in problems experienced by a device" (See, e.g., Nine, column 9, lines 30-33). However, Nine does not disclose specifically

how such patterns are detected. In particular, Nine does not disclose that patterns are detected by updating a threshold similarity requirement or a similarity expectation for alert features. In fact, Nine does not disclose the use of any kind of threshold or the updating of any kind of feature-related metric. As such, the Applicants respectfully submit that the Examiner is reading far more into Nine than is supported by Nine's disclosure.

Thus, there is simply no support in Nine for the steps of updating or otherwise implementing: (1) a threshold similarity requirement for one or more features of an alert relative to features of alert classes; or (2) a similarity expectation for one or more features of an alert relative to features of alert classes.

### **3. "Associating the new alert with the existing alert class that the new alert most closely matches"**

The Applicants submit that Nine is completely devoid of any teaching, showing, or suggestion relating to associating a new alert with the existing alert class that the new alert most closely matches, as claimed by the Applicants in independent claims 1, 7, and 13. The portion of Nine that the Examiner cites to teach this feature in fact merely teaches three techniques for detecting a problem with a monitored service. The first technique checks to make sure that the service is responsive (e.g., by "ping, nmap, finger, or telnet", Nine at column 7, lines 25-33). The second technique monitors environmental sensors to detect problems with the environment (e.g., "if the temperature is too high", Nine at column 7, lines 34-39). The third technique examines a log of the monitored service and parses for potential problems (e.g., indication that a particular route associated with a router is not functioning, Nine at column 7, lines 40-46). None of these techniques involve the comparison of an alert to existing alert classes, or the association of the alert with one of the existing alert classes based on the comparison.

### **4. "Defining a new alert class that is associated with the new alert"**

The Applicants submit that Nine is completely devoid of any teaching, showing, or suggestion relating to associating a new alert with a newly defined alert class when

the new alert fails to match an existing alert class, as claimed by the Applicants in independent claims 1, 7, and 13. The portion of Nine that the Examiner cites to teach this feature in fact merely teaches that log files for a monitored service may be used to diagnose problems with the service. Again, there is no mention of the need to compare an alert with existing alert classes in order to classify the alert, as claimed by the Applicants. Additionally, Nine discloses nothing about defining a new class when an alert fails to match an existing class. At best, Nine discloses generating a new report based on information extracted from logged tickets (such as total number of tickets). However, the generation of the report has nothing to do with the attempted classification of a particular ticket or alert.

**5. "Identifying a set of similar features shared by the new alert and one or more existing alert classes"**

The Applicants submit that Nine is completely devoid of any teaching, showing, or suggestion relating to classifying an alert in accordance with its features, as claimed by the Applicants in independent claims 1, 7, and 13. The portion of Nine that the Examiner cites to teach this feature in actuality merely teaches that software monitors a service and reports to the NOS when the service is unresponsive or when an anomaly is detected. The report contains "information about the service, such as location, severity of the problem, and time of occurrence" (See, e.g., Nine at column 3, lines 12-20). There is no mention in this passage of the need to identify features of the problem or to compare the problem to other known problems (e.g., existing alert classes) based on the identified features.

In short, as discussed above, Nine fails to teach, show, or suggest any sort of classification of alerts by comparing features of the alerts to features of existing alert classes, as recited by the Applicants in independent claims 1, 7, and 13. Moreover, the Applicants respectfully submit that the explicit teachings of Nine actually teach away from the claimed classification step. Specifically, Nine teaches that an additional reporting feature is required to detect groups of tickets related to a common problem (See, e.g., Nine, column 9, lines 30-39: "if a series of tickets indicate that a security log

file on an NT server has a flood of ICMP packets, a report may be created to locate all of the tickets that indicate this problem," emphasis added). If the tickets had been classified (*i.e.*, compared against other tickets and grouped together into classes) as they were generated (*i.e.*, before being transmitted to the appropriate location), then such a report would not be necessary. That is, all of the tickets that indicate the problem would already be grouped together. Thus, the post-transmission reporting feature required by Nine clearly indicates that Nine teaches that the tickets are not classified or compared to each other, as claimed by the Applicants.

Specifically, Applicants' claims 1, 7, and 13 positively recite:

1. In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, the method comprising:

- (a) receiving a new alert;
- (b) identifying a set of similar features shared by the new alert and one or more existing alert classes;
- (c) updating a threshold similarity requirement for one or more of the similar features;
- (d) updating a similarity expectation for one or more of the similar features;
- (e) comparing the new alert with the one or more existing alert classes; and either:
- (f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or
- (f2) defining a new alert class that is associated with the new alert. (Emphasis added)

7. A computer readable medium containing an executable program for organizing alerts that are generated by a plurality of sensors into alert classes, both the alerts and the alert classes having a plurality of features, where the program causes a processor to perform steps of:

- (a) receiving a new alert;
- (b) identifying a set of similar features shared by the new alert and one or more existing alert classes;
- (c) updating a threshold similarity requirement for one or more of the similar features;
- (d) updating a similarity expectation for one or more of the similar features;
- (e) comparing the new alert with the one or more existing alert classes; and either:
- (f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or
- (f2) defining a new alert class that is associated with the new alert. (Emphasis added)

13. In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, where the system comprises:

(a) means for receiving a new alert;

(b) means for identifying a set of similar features shared by the new alert and one or more existing alert classes;

(c) means for updating a threshold similarity requirement for one or more of the similar features;

(d) means for updating a similarity expectation for one or more of the similar features;

(e) means for comparing the new alert with the one or more existing alert classes; and

(f1) means for associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches, or defining a new alert class that is associated with the new alert. (Emphasis added)

As discussed above, nowhere does Nine teach or even suggest the desirability of classifying of alerts by comparing features of the alerts to features of existing alert classes. Moreover, even assuming for the sake of argument that the disclosure of Nine can be interpreted as teaching the classification of alerts, Nine fails to teach or suggest several other claimed features of the present invention, namely, the steps of updating a threshold similarity expectation for one or more features of an alert relative to features of alert classes and of updating a similarity expectation for one or more features. Therefore, the Applicants submit that independent claims 1, 7, and 13 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claims 2, 8, and 14 depend, respectively, from claims 1, 7, and 13, and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2, 8, and 14 are not anticipated by the teachings of Nine. Therefore, the Applicants submit that dependent claims 2, 8, and 14 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

In light of the above, the Applicants respectfully request that the rejection of claims 1-2, 7-8, and 13-14 under 35 U.S.C. §102 be withdrawn.

## **B. Claims 7-8**

Claims 7-8 stand rejected as being unpatentable over the Baggen patent (U.S. 4,667,317, issued May 19, 1987, hereinafter "Baggen"). In response, the Applicants have amended independent claim 7 in order to more clearly recite aspects of the present invention.

In particular, the Applicants have amended independent claim 7, in accordance with the Examiner's suggestion, to recite that the claimed program "causes a processor to perform steps of: receiving ... identifying ... updating a threshold similarity ... updating a similarity expectation ... comparing ... associating ... and defining ...." The Examiner indicated in the Final Office Action that such an amendment "would make the claims distinguishable from a generic computer readable medium with data," as allegedly disclosed by Baggen. As such, the Applicants respectfully submit that independent claim 7 is not anticipated by Baggen.

Dependent claim 8 depends from independent claim 7 and recites additional features. As such, and for at least the same reasons set forth above, the Applicants submit that claim 8 is not anticipated by Baggen.

In light of the above, the Applicants respectfully request that the rejection of claims 7-8 under 35 U.S.C. §102 be withdrawn.

## **III. VOLUNTARY CLAIM AMENDMENTS**

The Applicants have voluntarily amended several of the claims in order to correct minor typographical errors. The Applicants do not believe that these amendments substantively alter the scope of the pending claims.

## **IV. CONCLUSION**

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §101 and 35 U.S.C. §102. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring


09/944,788

the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Kin-Wah Tong, Esq. at (732) 842-8110 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

May 18, 2010

Date

  
\_\_\_\_\_  
Kin-Wah Tong, Attorney  
Reg. No. 39,400  
(732) 842-8110

Wall & Tong, LLP  
595 Shrewsbury Avenue  
Shrewsbury, New Jersey 07702